UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF MICHIGAN

ZACHARY KNAPP, on behalf of himself and all others similarly situated, Plaintiff, v. **ALBION COLLEGE,** Defendant.	No. **CLASS ACTION COMPLAINT** **DEMAND FOR JURY TRIAL**

Zachary Knapp ("Plaintiff"), through his attorneys, individually and on behalf of all others similarly situated, brings this Class Action Complaint against Defendant Albion College ("Albion" or "Defendant"), and its present, former, or future direct and indirect parent companies, subsidiaries, affiliates, agents, and/or other related entities. Plaintiff alleges the following on information and belief—except as to his own actions, counsel's investigations, and facts of public record.

NATURE OF ACTION

1. This class action arises from Defendant's failure to protect highly sensitive data.

2. Defendant is a liberal arts college based in Albion, Michigan.[1]

3. As such, Defendant stores a litany of highly sensitive personal identifiable information ("PII") about its current and former employees and students. But Defendant lost control over that data when cybercriminals infiltrated its insufficiently protected computer systems in a data breach (the "Data Breach").

[1] *About*, ALBION, https://www.albion.edu/about/ (last visited May 12, 2025).

4. It is unknown for precisely how long the cybercriminals had access to Defendant's network before the breach was discovered. In other words, Defendant had no effective means to prevent, detect, stop, or mitigate breaches of its systems—thereby allowing cybercriminals unrestricted access to its current and former employees' and students' PII.

5. On information and belief, cybercriminals were able to breach Defendant's systems because Defendant failed to adequately train its employees on cybersecurity and failed to maintain reasonable security safeguards or protocols to protect the Class's PII. In short, Defendant's failures placed the Class's PII in a vulnerable position—rendering them easy targets for cybercriminals.

6. Plaintiff is a Data Breach victim, having received a notice letter from Defendant about the Data Breach ("Breach Notice"), which is attached as Exhibit A. He brings this class action on behalf of himself, and all others harmed by Defendant's misconduct.

7. The exposure of one's PII to cybercriminals is a bell that cannot be unrung. Before this data breach, its current and former employees' and students' private information was exactly that—private. Not anymore. Now, their private information is forever exposed and unsecure.

PARTIES

8. Plaintiff, Zachary Knapp, is a natural person and citizen of Michigan where he intends to remain.

9. Defendant, Albion College, is a domestic nonprofit corporation incorporated under the laws of Michigan with its principal place of business at 611 E. Porter, St.. Albion, MI, 49224.

JURISDICTION AND VENUE

10. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of

interest and costs. Defendant and at least one class member are citizens of different states and there are over 100 putative Class Members.

11. Many states, including Maine and Texas, have statutes requiring organizations to report data breaches to the state government. *See* M.R.S. § 1348; Tex. Bus. & Com. Code §§ 521.053.

12. Pursuant to M.R.S. § 1348, Defendant submitted a sample letter and submitted other information about the Data Breach to the Maine Attorney General's Office, which is publicly available[2] and attached hereto as Exhibit B. Defendant reported that 3 Maine residents were affected by the Data Breach.[3]

13. Pursuant to Tex. Bus. & Com. Code §§ 521.053, Defendant submitted information about the Data Breach to the Texas Attorney General's Office, which is publicly available.[4] Defendant reported that 275 Texas residents were affected by the Data Breach.[5]

14. Because Defendant has publicly reported the existence of numerous members of the proposed class in states other than Michigan, Plaintiff has satisfied the minimal jurisdictional requirements set forth in 28 U.S.C. § 1332(d)(2) in that there are members of the putative class in foreign states different from Defendant.

[2] *Data Breach Notification*, OFFICE OF THE MAINE ATTORNEY GENERAL, https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/d16941f7-1e1e-4625-9a16-437a13f4f948.html (last visited May 12, 2025).
[3] *Id.*
[4] *Data Security Breach Reports*, ATTORNEY GENERAL OF TEXAS, https://oag.my.site.com/datasecuritybreachreport/apex/DataSecurityReportsPage (last visited May 12, 2025).
[5] *Id.*

15. This Court has personal jurisdiction over Defendant because it is headquartered in Michigan, regularly conducts business in Michigan, and has sufficient minimum contacts in Michigan.

16. Venue is proper in this Court because Defendant's principal office is in this District, and because a substantial part of the events, acts, and omissions giving rise to Plaintiff's claims occurred in this District.

BACKGROUND

Defendant Collected and Stored the PII of Plaintiff and the Class

17. Albion is college that states it is "nationally recognized for its academic excellence in the liberal arts tradition, a learning-centered commitment, and a future-oriented perspective."[6]

18. Albion enrolls 1,354 students[7], states it has an alumni network of over 32,000[8], and has 23 academic departments offering its students 73 majors.[9]

19. Thus, as part of its operations, Albion receives and maintains the PII of thousands of its current and former employees and students.

20. In collecting and maintaining the PII, Defendant agreed it would safeguard the data in accordance with its internal policies, state law, and federal law. After all, Plaintiff and Class Members themselves took reasonable steps to secure their PII.

21. Under state and federal law, organizations like Defendant have duties to protect its current and former employees' and students' PII and to notify them about breaches.

---

[6] *Mission, Vision, and Values*, ALBION, https://www.albion.edu/about/mission/ (last visited May 12, 2025).
[7] *Albion at a Glance*, ALBION, https://www.albion.edu/about/at-a-glance/ (last visited May 12, 2025).
[8] *Id.*
[9] *Key Facts*, ALBION, https://www.albion.edu/about/at-a-glance/key-facts/ (last visited May 12, 2025).

22. Defendant recognized these duties in its "Data Privacy Policy," promising:

a. "Albion College ("the College") is committed to maintaining the privacy, integrity, security and availability of confidential information created, received, maintained and/or stored by the College, regardless of form;"

b. "Confidential information and records are to be accessed, used and disclosed only with explicit authorization, in accordance with applicable law, and on a need–to–know basis related to a College function. Such information must never be disclosed outside of the College without express authorization;"

c. "To help users appropriately secure and manage Confidential information and records, the College has adopted various Data Standards set by the State of Michigan (safecomputing.umich.edu), that, among other things, categorizes data by sensitivity and risk level and designates roles and responsibilities for data use and management."[10]

23. Despite recognizing its duty to do so, on information and belief, Albion did not implement reasonably cybersecurity safeguards or policies to protect its employees' and students' PII or supervise its IT or data security agents and employees to prevent, detect, and stop breaches of its systems. As a result, Albion leaves significant vulnerabilities in its systems for cybercriminals to exploit and gain access to the PII in its possession.

Albion's Data Breach

[10] *Data Privacy Policy*, ALBION, https://www.albion.edu/offices/information-technology/support/data-privacy-policy/ (last visited May 12, 2025).

24. Defendant discovered "unauthorized access" to its network on December 17, 2024.[11]

25. Due to the obfuscating language in Albion's Breach Noice, it is unclear when or how the Data Breach occurred, what information was impacted, or how Albion discovered the breach. However, Defendant admits that it launched an investigation and, on April 18, 2025, determined that Plaintiff's name and Social Security number were "removed from our network."[12]

26. Defendant reported to the Attorney General of Texas that the below types of PII were compromised in the Data Breach:

a. Social Security numbers;

b. Government issued ID numbers (*e.g.* passport, state ID card);

c. Financial Information (*e.g.* account number, credit or debit card number); and

d. Medical Information.[13]

27. And yet, Defendant waited over until May 1, 2025, 13 days after it stated that Plaintiff's PII was compromised, before it began notifying the class—almost ***135 days*** after the Data Breach began.

28. Thus, Defendant kept the Class in the dark—thereby depriving the Class of the opportunity to try and mitigate their injuries in a timely manner.

29. And when Defendant did notify Plaintiff and the Class of the Data Breach, Defendant acknowledged that the Data Breach created a present, continuing, and significant risk of suffering identity theft, warning Plaintiff and the Class:

[11] Ex. A.
[12] *Id*.
[13] N. 4.

a. "This letter also provides other precautionary measures you can take to protect your personal information, including placing a Fraud Alert and/or Security Freeze on your credit files, and/or obtaining a free credit report;"

b. "[R]emain vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis."[14]

30. Defendant failed its duties when its inadequate security practices caused the Data Breach. In other words, Defendant's negligence is evidenced by its failure to prevent the Data Breach and stop cybercriminals from accessing the PII. And thus, Defendant caused widespread injury and monetary damages.

31. Since the breach, Defendant claims it is "committed to maintaining the privacy of personal information in [its] possession and [has] taken many precautions to safeguard it."[15] However, such simple declarations are insufficient to ensure that Plaintiff's and Class Members' PII will be protected from additional exposure in a subsequent data breach.

32. Further, Albion's Breach Notice shows that it cannot—or will not—determine the full scope of the Data Breach, as Defendant has been unable to determine precisely when the Data Breach began and ended.

33. Defendant has done little to remedy its Data Breach. True, Defendant has offered some victims credit monitoring and identity related services. But upon information and belief, such services are wholly insufficient to compensate Plaintiff and Class Members for the injuries that Defendant inflicted upon them.

[14] Ex. B.
[15] *Id.*

34. Because of Defendant's Data Breach, the sensitive PII of Plaintiff and Class Members was placed into the hands of cybercriminals—inflicting numerous injuries and significant damages upon Plaintiff and Class Members.

35. Indeed, numerous cybersecurity firms who track dark web activity have reported that the hacker group "Medusa" has taken credit for the Data Breach.[16, 17]

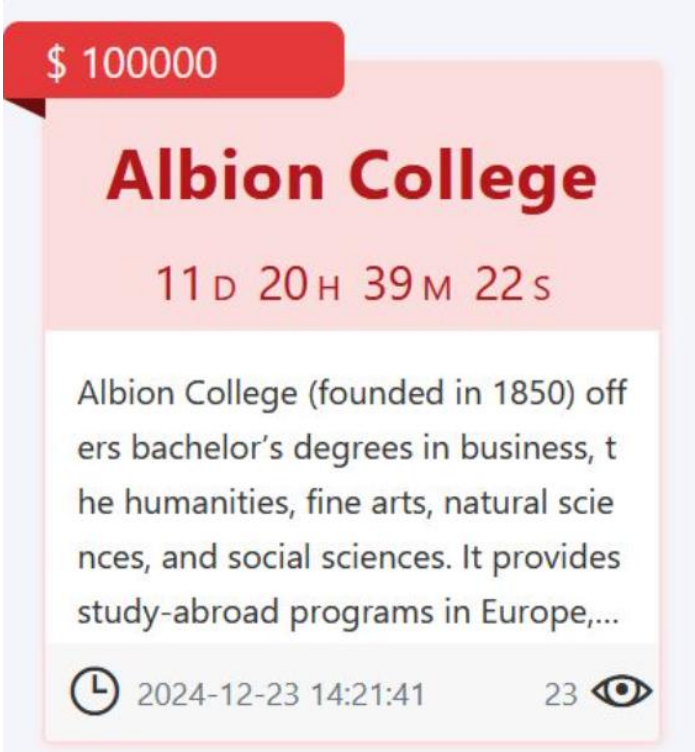
36. Medusa is a cyber gang that, according to the United States' Cybersecurity and Infrastructure Security Agency ("CISA"), operates a double extortion model, where a organization's files are encrypted and *exfiltrated* to Medusa's servers.[18] Organizations then must pay to decrypt the stolen files and prevent their release.[19]

37. CISA further advises that Medusa has expanded to an "affiliate model" where affiliates, referred to as "Medusa actors," use the group's software to attack organizations and take a cut of the resulting extortion payments.[20]

38. On December 23, 2024, Medusa created a post on its dark web website[21] indicating that it had hacked Defendant and stolen PII from its computer network.[22]

---

[16] *HACK TUESDAY WEEK 18 – 24 DECEMBER* 2024, HACKMANAC, https://hackmanac.com/news/hack-tuesday-week-18-24-december-2024 (last visited May 12, 2025).
[17] *[MEDUSA] – Ransomware Victim: Albion College*, REDPACKET SECURITY (Dec. 23, 2024), https://www.redpacketsecurity.com/medusa-ransomware-victim-albion-college/.
[18] *#StopRansomware: Medusa Ransomware*, CISA (Mar. 12, 2025), https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-071a.
[19] *Id.*
[20] *Id.*
[21] The screen shot regarding the dark web post related to the Data Breach was obtained from Falcon Feeds, a firm providing cybersecurity and dark web and ransomware monitoring services. *See Home Page*, FALCON FEEDS, https://falconfeeds.io/ (last visited May 10, 2025).
[22] @FalconFeeds.io, Twitter (X) (December 23, 2024, 10:47 AM) https://bsky.app/profile/falconfeedsio.bsky.social/post/3ldyf2p6lls2z.



39. Medusa's post listed a price of "$10,000" and a countdown clock stating "11 D, 20 H, 39 M , 22 S" indicating Albion's data would be published if Albion did not make a ransom payment within that time period.[23]

40. CISA has confirmed that this is Medusa's *modus operandi*, stating in its advisory that "Medusa operates a [dark web] data leak site, divulging victims alongside countdowns to the release of information. Ransom demands are posted on the site, with direct hyperlinks to Medusa affiliated cryptocurrency wallets. At this stage, *Medusa concurrently advertises sale of the data to interested parties before the countdown timer ends*. Victims can additionally pay $10,000 USD in cryptocurrency to add a day to the countdown timer."[24]

[23] *Id*.
[24] N. 18 (emphasis added).

41. Defendant has not made any public statements on whether it made a ransom payment to Medusa related to the Data Breach.

42. Thus, on information and belief, Plaintiff's and Class Members' PII has already been published, or will be published imminently, on the dark web.

43. Moreover, even if Albion made a ransom payment, there is no guarantee that the data Medusa stole will be deleted.[25] The stolen PII is valuable, and can easily be sold to another threat actor, so there is little incentive to delete it.[26] As the CISA advisory indicated *supra*, Medusa advertises the sale of the data it steals to anyone willing to pay concurrently with its ransom demands.

44. In addition, according to the CISA advisory, FBI investigations identified that after paying the ransom, one victim was contacted by a separate Medusa actor who claimed the negotiator had stolen the ransom amount already paid and requested half of the payment be made again to provide the "true decryptor."[27] This indicates that the "Medusa actors" will not abide by Medusa's promises not to disclose an organization's data after a ransom payment has been made.

45. Further, there have been cases where the links that lead to compromised files, while removed from the group who received the ransom payment's dark web website, remain available on the servers used by other hackers, even after the demand is met.[28]

46. Cybercriminal groups can monetize stolen PII and sell it on the dark web as part of

[25] Steve Adler, *Majority of Ransomware Victims That Pay a Ransom Suffer a Second Attack*, THE HIPAA JOURNAL (Feb. 23, 2024), https://www.hipaajournal.com/majority-of-ransomware-victims-that-pay-a-ransom-suffer-a-second-attack/.
[26] *Id*.
[27] N. 18.
[28] *Dedicated Leak Sites (DLS): Here's what you should know*, Group-IB, https://www.group-ib.com/resources/knowledge-hub/dedicated-leak-sites/ (last visited Apr. 22, 2025).

a full identity profile.[29] Buyers can then use that information to conduct different types of identity theft or fraud, such as filing a fake tax return, applying for a fraudulent mortgage or opening a bank account while impersonating the victim.[30]

47. To date, on information and belief, Defendant has not notified Plaintiff and Class Members about the theft of their PII by Medusa, leaving them vulnerable to identity theft and fraud.

48. As a result of Albion's omissions, Plaintiff's and Class Members' ability to mitigate the harms resulting from the Data Breach has been severely impaired.

49. Upon information and belief, the Medusa cybercriminal group was able to: (1) defeat Albion's security systems, (2) gain access to its network and gain access to the sensitive PII contained therein, and (3) successfully steal Plaintiff's and the Class's PII.

50. And as the Harvard Business Review notes, such "[c]ybercriminals frequently use the Dark Web—a hub of criminal and illicit activity—to sell data from companies that they have gained unauthorized access to through credential stuffing attacks, phishing attacks, [or] hacking."[31]

51. Defendant, a sophisticated actor with that states it strives to ensure data integrity,[32] knew or should have known of the tactics that groups like Medusa employ.

Plaintiff's Experiences and Injuries

---

[29] Anthony M. Freed, *Which Data Do Ransomware Attackers Target for Double Extortion?*, MALICIOUSLIFE BY CYBEREASON, https://www.cybereason.com/blog/which-data-do-ransomware-attackers-target-for-double-extortion (listed visited Mar. 6, 2025).

[30] *Id*.

[31] Brenda R. Sharton, *Your Company's Data Is for Sale on the Dark Web. Should You Buy It Back?*, HARVARD BUS. REV. (Jan. 4, 2023) https://hbr.org/2023/01/your-companys-data-is-for-sale-on-the-dark-web-should-you-buy-it-back.

[32] *Information Technology*, ALBION, https://www.albion.edu/offices/information-technology/ (last visited May 12, 2025).

52. Plaintiff Zachary Knapp is a former student of Defendant. Plaintiff received a personalized Data Breach notice explaining that his PII was exposed in Defendant's Data Breach.[33]

53. As a result, Plaintiff was injured by Defendant's Data Breach.

54. As a condition of enrolling as a student at Albion, Defendant obtained Plaintiff's PII and used that PII to facilitate its operations.

55. Plaintiff provided his PII to Defendant and trusted the college would use reasonable measures to protect it according to Defendant's internal policies, as well as state and federal law. Defendant obtained and continues to maintain Plaintiff's PII and has a continuing legal duty and obligation to protect that PII from unauthorized access and disclosure.

56. Plaintiff reasonably understood that a portion of the funds derived from his tuition payments to Albion would be used to pay for adequate cybersecurity and protection of PII.

57. Plaintiff received a Notice of Data Breach on or around May 8, 2025.

58. Thus, on information and belief, Plaintiff's PII has already been published—or will be published imminently—by Medusa or other cybercriminals on the dark web.

59. Through its Data Breach, Defendant compromised Plaintiff's PII, including but not limited to his name and Social Security number.[34] However, based on Albion's report to the Attorney General of Texas, additional PII, such as Plaintiff's financial and/or driver's license information, may have also been stolen by Medusa in the Data Breach.

60. To the best of his knowledge, Plaintiff has not been the victim of another data breach, except for the Data Breach at issue here.

[33] Ex. A.
[34] *Id.*

61. Since the Data Breach, Plaintiff has experienced a dramatic increase in scam and phishing texts and emails purporting to be from the IRS and asking him to follow links related to his tax returns. This suggests that his PII has already been placed in the hands of cybercriminals.

62. On information and belief, Plaintiff's email address and phone number was compromised as a result of the Data Breach, as cybercriminals are able to use an individual's PII that is accessible on the dark web, as Plaintiff's is here, to gather and steal even more information.

63. Plaintiff estimates he has spent approximately 5 hours addressing the Data Breach. This includes time researching the Data Breach, time monitoring his accounts to protect himself from identity theft, and time attempting to sign up for the credit monitoring service offered by Defendant in its Breach Notice. After all, Defendant directed Plaintiff to take those steps in its Breach Notice.

64. Plaintiff has been unable to sign up for the credit monitoring offered in Albion's Data Breach as the link contained in its Breach Notice was inoperable.

65. Plaintiff fears for his personal financial security and worries about what information was exposed in the Data Breach.

66. Because of Defendant's Data Breach, Plaintiff has suffered—and will continue to suffer from—anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond allegations of mere worry or inconvenience. Rather, Plaintiff's injuries are precisely the type of injuries that the law contemplates and addresses.

67. Plaintiff suffered actual injury from the exposure and theft of his PII—which violates his rights to privacy.

68. Plaintiff suffered actual injury in the form of damages to and diminution in the value of his PII. After all, PII is a form of intangible property—property that Defendant was required to adequately protect.

69. Plaintiff suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because Defendant's Data Breach placed Plaintiff's PII right in the hands of criminals.

70. Because of the Data Breach, Plaintiff anticipates spending considerable amounts of time and money to try and mitigate his injuries.

71. Today, Plaintiff has a continuing interest in ensuring that his PII—which, upon information and belief, remains backed up in Defendant's possession—is protected and safeguarded from additional breaches.

Plaintiff and the Proposed Class Face Significant Risk of Continued Identity Theft

72. Because of Defendant's failure to prevent the Data Breach, Plaintiff and Class Members suffered—and will continue to suffer—damages. These damages include, *inter alia*, monetary losses, lost time, anxiety, and emotional distress. Also, they suffered or are at an increased risk of suffering:

a. loss of the opportunity to control how their PII is used;

b. diminution in value of their PII;

c. compromise and continuing publication of their PII;

d. out-of-pocket costs from trying to prevent, detect, and recovery from identity theft and fraud;

e. lost opportunity costs and wages from spending time trying to mitigate the fallout of the Data Breach by, *inter alia*, preventing, detecting, contesting, and recovering from identify theft and fraud;

f. delay in receipt of tax refund monies;

g. unauthorized use of their stolen PII; and

h. continued risk to their PII—which remains in Defendant's possession—and is thus as risk for futures breaches so long as Defendant fails to take appropriate measures to protect the PII.

73. Stolen PII is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen PII can be worth up to $1,000.00 depending on the type of information obtained.

74. The value of Plaintiff and Class's PII on the black market is considerable. Stolen PII trades on the black market for years. And criminals frequently post and sell stolen information openly and directly on the "Dark Web"—further exposing the information.

75. It can take victims years to discover such identity theft and fraud. This gives criminals plenty of time to sell the PII far and wide.

76. One way that criminals profit from stolen PII is by creating comprehensive dossiers on individuals called "Fullz" packages. These dossiers are both shockingly accurate and comprehensive. Criminals create them by cross-referencing and combining two sources of data—first the stolen PII, and second, unregulated data found elsewhere on the internet (like phone numbers, emails, addresses, etc.).

77. The development of "Fullz" packages means that the PII exposed in the Data Breach can easily be linked to data of Plaintiff and the Class that is available on the internet.

78. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiff and Class Members, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff and other Class Members' stolen PII is being misused, and that such misuse is fairly traceable to the Data Breach.

79. Defendant disclosed the PII of Plaintiff and Class Members for criminals to use in the conduct of criminal activity. Specifically, Defendant opened up, disclosed, and exposed the PII of Plaintiff and Class Members to people engaged in disruptive and unlawful business practices and tactics, including online account hacking, unauthorized use of financial accounts, and fraudulent attempts to open unauthorized financial accounts (i.e., identity fraud), all using the stolen PII.

80. Defendant's failure to promptly and properly notify Plaintiff and Class Members of the Data Breach exacerbated Plaintiff and Class Members' injury by depriving them of the earliest ability to take appropriate measures to protect their PII and take other necessary steps to mitigate the harm caused by the Data Breach.

Defendant Knew—Or Should Have Known—of the Risk of a Data Breach

81. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in recent years.

82. In 2021, a record 1,862 data breaches occurred, exposing approximately

293,927,708 sensitive records—a 68% increase from 2020.[35] Of the 1,862 recorded data breaches, 330 of them, or 17.7% were in the medical or healthcare industry.[36] Those 330 reported breaches exposed nearly 30 million sensitive records (28,045,658), compared to only 306 breaches that exposed nearly 10 million sensitive records (9,700,238) in 2020.[37]

83. Indeed, cyberattacks have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service issue warnings to potential targets, so they are aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive to ransomware criminals . . . because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[38]

84. In fact, according to the cybersecurity firm Mimecast, 90% of healthcare organizations experienced cyberattacks in the past year.[39]

85. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendant's industry, including Defendant.

Defendant Failed to Follow FTC Guidelines

86. According to the Federal Trade Commission ("FTC"), the need for data security should be factored into all business decision-making. Thus, the FTC issued numerous guidelines

---

[35] *See 2021 Data Breach Annual Report*, IDENTITY THEFT RESOURCE CENTER (Jan. 2022) https://notified.idtheftcenter.org/s/.

[36] *Id*.

[37] *Id*.

[38] Ben Kochman, *FBI, Secret Service Warn of Targeted Ransomware*, LAW360 (Nov. 18, 2019), https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware.

[39] *See* Maria Henriquez, *Iowa City Hospital Suffers Phishing Attack*, SECURITY MAGAZINE (Nov. 23, 2020), https://www.securitymagazine.com/articles/93988-iowa-city-hospital-suffers-phishing-attack (last visited Feb. 19, 2025).

identifying best data security practices that businesses—like Defendant—should use to protect against unlawful data exposure.

87. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*. There, the FTC set guidelines for what data security principles and practices businesses must use.[40] The FTC declared that, *inter alia*, businesses must:

a. protect the personal customer information that they keep;

b. properly dispose of personal information that is no longer needed;

c. encrypt information stored on computer networks;

d. understand their network's vulnerabilities; and

e. implement policies to correct security problems.

88. The guidelines also recommend that businesses watch for the transmission of large amounts of data out of the system—and then have a response plan ready for such a breach.

89. Furthermore, the FTC explains that companies must:

a. not maintain information longer than is needed to authorize a transaction;

b. limit access to sensitive data;

c. require complex passwords to be used on networks;

d. use industry-tested methods for security;

e. monitor for suspicious activity on the network; and

f. verify that third-party service providers use reasonable security measures.

90. The FTC brings enforcement actions against businesses for failing to protect customer data adequately and reasonably. Thus, the FTC treats the failure—to use reasonable and

[40] *Protecting Personal Information: A Guide for Business*, FED TRADE COMMISSION (Oct. 2016) https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

appropriate measures to protect against unauthorized access to confidential consumer data—as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

91. In short, Defendant's failure to use reasonable and appropriate measures to protect against unauthorized access to its current and former employees' and students' data constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

Defendant Failed to Follow Industry Standards

92. Several best practices have been identified that—at a *minimum*—should be implemented by businesses like Defendant. These industry standards include: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption (making data unreadable without a key); multi-factor authentication; backup data; and limiting which employees can access sensitive data.

93. Other industry standard best practices include: installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.

94. Upon information and belief, Defendant failed to implement industry-standard cybersecurity measures, including failing to meet the minimum standards of both the NIST Cybersecurity Framework Version 2.0 (including without limitation PR.AA-01, PR.AA.-02, PR.AA-03, PR.AA-04, PR.AA-05, PR.AT-01, PR.DS-01, PR-DS-02, PR.DS-10, PR.PS-01, PR.PS-02, PR.PS-05, PR.IR-01, DE.CM-01, DE.CM-03, DE.CM-06, DE.CM-09, and RS.CO-04)

and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

95. These frameworks are applicable and accepted industry standards. And by failing to comply with these accepted standards, Defendant opened the door to the criminals—thereby causing the Data Breach.

CLASS ACTION ALLEGATIONS

96. Plaintiff brings this class action under Fed. R. Civ. P. 23(a), 23(b)(2), and 23(b)(3), individually and on behalf of all members of the following class:

> All individuals residing in the United States whose PII was compromised in the Data Breach, including all those individuals who received notice of the Data Breach.

97. Excluded from the Class are Defendant, its agents, affiliates, parents, subsidiaries, any entity in which Defendant has a controlling interest, any Defendant officer or director, any successor or assign, and any Judge who adjudicates this case, including their staff and immediate family.

98. Plaintiff reserves the right to amend the class definition.

99. Plaintiff and Class Members constitute a well-defined community of interest—they are similarly situated persons and were similarly affected and damaged by the alleged conduct of Defendant.

100. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of his claims on class-wide bases using the same evidence as would be used to prove those elements in individual actions asserting the same claims.

101. Ascertainability. All members of the proposed Class are readily ascertainable from information in Defendant's custody and control. After all, Defendant already identified some individuals and sent them data breach notices.

102. Numerosity. The Class Members are so numerous that joinder of all Class Members is impracticable. Upon information and belief, the proposed Class includes at least thousands of members.

103. Typicality. Plaintiff's claims are typical of Class Members' claims as each arises from the same Data Breach, the same alleged violations by Defendant, and the same unreasonable manner of notifying individuals about the Data Breach.

104. Adequacy. Plaintiff will fairly and adequately protect the proposed Class's common interests. His interests do not conflict with Class Members' interests. And Plaintiff has retained counsel—including lead counsel—that is experienced in complex class action litigation and data privacy to prosecute this action on the Class's behalf.

105. Commonality and Predominance. Plaintiff's and the Class's claims raise predominantly common fact and legal questions—which predominate over any questions affecting individual Class Members—for which a class wide proceeding can answer for all Class Members. In fact, a class wide proceeding is necessary to answer the following questions:

a. if Defendant had a duty to use reasonable care in safeguarding Plaintiff's and the Class's PII;

b. if Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. if Defendant were negligent in maintaining, protecting, and securing PII;

d. if Defendant breached contract promises to safeguard Plaintiff and the Class's PII;

e. if Defendant took reasonable measures to determine the extent of the Data Breach after discovering it;

f. if Defendant's Breach Notice was reasonable;

g. if the Data Breach caused Plaintiff and the Class injuries;

h. what the proper damages measure is; and

i. if Plaintiff and the Class are entitled to damages, treble damages, and or injunctive relief.

106. Superiority. A class action will provide substantial benefits and is superior to all other available means for the fair and efficient adjudication of this controversy. The damages or other financial detriment suffered by individual Class Members are relatively small compared to the burden and expense that individual litigation against Defendant would require. Thus, it would be practically impossible for Class Members, on an individual basis, to obtain effective redress for their injuries. Not only would individualized litigation increase the delay and expense to all parties and the courts, but individualized litigation would also create the danger of inconsistent or contradictory judgments arising from the same set of facts. By contrast, the class action device provides the benefits of adjudication of these issues in a single proceeding, ensures economies of scale, provides comprehensive supervision by a single court, and presents no unusual management difficulties.

COUNT I
Negligence
(On Behalf of Plaintiff and the Class)

107. Plaintiff and members of the Class incorporate the above allegations as if fully set forth herein.

108. Defendant owed to Plaintiff and the Class a duty to exercise reasonable care in handling and using the PII in its care and custody, including implementing industry-standard security procedures sufficient to reasonably protect the information from the Data Breach, theft, and unauthorized use that came to pass, and to promptly detect attempts at unauthorized access.

109. Defendant owed a duty of care to Plaintiff and members of the Class because it was foreseeable that Defendant's failure to adequately safeguard their PII in accordance with state-of-the-art industry standards concerning data security would result in the compromise of that PII—just like the Data Breach that ultimately came to pass. Defendant acted with wanton and reckless disregard for the security and confidentiality of Plaintiff's and members of the Class's PII by disclosing and providing access to this information to third parties and by failing to properly supervise both the way the PII was stored, used, and exchanged, and those in its employ who were responsible for making that happen.

110. Defendant owed to Plaintiff and members of the Class a duty to notify them within a reasonable timeframe of any breach to the security of their PII. Defendant also owed a duty to timely and accurately disclose to Plaintiff and members of the Class the scope, nature, and occurrence of the Data Breach. This duty is required and necessary for Plaintiff and members of the Class to take appropriate measures to protect their PII, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the Data Breach.

111. Defendant owed these duties to Plaintiff and members of the Class because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendant knew or should have known would suffer injury-in-fact from Defendant's inadequate security protocols. Defendant actively sought and obtained Plaintiff's and the Class's personal information and PII.

112. The risk that unauthorized persons would attempt to gain access to the PII and misuse it was foreseeable. Given that Defendant holds vast amounts of PII, it was inevitable that unauthorized individuals would attempt to access Defendant's databases containing the PII—whether by malware or otherwise.

113. PII is highly valuable, and Defendant knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the PII of Plaintiff and members of the Class and the importance of exercising reasonable care in handling it.

114. Defendant breached its duties by failing to exercise reasonable care in handling and securing the personal information and PII of Plaintiff and members of the Class which actually and proximately caused the Data Breach and Plaintiff's and members of the Class's injury. Defendant further breached its duties by failing to provide reasonably timely notice of the Data Breach to Plaintiff and the Class, which actually and proximately caused and exacerbated the harm from the Data Breach and Plaintiff's and members of the Class's injuries-in-fact. As a direct and traceable result of Defendant's negligence and/or negligent supervision, Plaintiff and members of the Class have suffered or will suffer damages, including monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

115. Defendant's breach of its common-law duties to exercise reasonable care and its failures and negligence actually and proximately caused Plaintiff and members of the Class actual, tangible, injury-in-fact and damages, including, without limitation, the theft of their PII by criminals, improper disclosure of their PII, lost value of their PII, and lost time and money incurred to mitigate and remediate the effects of the Data Breach that resulted from and were caused by Defendant's negligence, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

COUNT II
Negligence *Per Se*
(On Behalf of Plaintiff and the Class)

116. Plaintiff and members of the Class incorporate the above allegations as if fully set forth herein.

117. Pursuant to the FTC Act, 15 U.S.C. § 45, Defendant has a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and members of the Class's PII.

118. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect employees' and students' PII. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendant's duty to protect Plaintiff's and the Class's sensitive PII.

119. Defendant violated its duty under Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII Defendant collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to individuals in the event of a breach, which ultimately came to pass.

120. The harm that has occurred is the type of harm the FTC Act is intended to guard against. Indeed, the FTC has pursued numerous enforcement actions against businesses that, because of its failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

121. Defendant has a duty to Plaintiff and the Class to implement and maintain

reasonable security procedures and practices to safeguard Plaintiff's and the Class's PII.

122. Defendant breached its duties to Plaintiff and members of the Class under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and members of the Class's PII.

123. Defendant's violation of Section 5 of the FTC Act and its failure to comply with applicable laws and regulations constitutes negligence *per se*.

124. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and members of the Class, Plaintiff and the Class would not have been injured.

125. The injury and harm suffered by Plaintiff and the Class were the reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should have known that it was failing to meet its duties and that its breach would cause Plaintiff and members of the Class to suffer the foreseeable harms associated with the exposure of their PII.

126. As a direct and proximate result of Defendant's negligence *per se*, Plaintiff and the Class have suffered harm, including loss of time and money resolving fraudulent charges; loss of time and money obtaining protections against future identity theft; lost control over the value of PII; harm resulting from damaged credit scores and information; and other harm resulting from the unauthorized use or threat of unauthorized use of stolen personal information, entitling them to damages in an amount to be proven at trial.

COUNT III
Breach of Fiduciary Duty
(On Behalf of Plaintiff and the Class)

127. Plaintiff and members of the Class incorporate the above allegations as if fully set forth herein.

128. Given the relationship between Defendant and Plaintiff and Class Members, where Defendant became guardian of Plaintiff's and Class Members' PII, Defendant became a fiduciary

by its undertaking and guardianship of the PII, to act primarily for Plaintiff and Class Members, (1) for the safeguarding of Plaintiff's and Class Members' PII; (2) to timely notify Plaintiff and Class Members of a Data Breach and disclosure; and (3) to maintain complete and accurate records of what information (and where) Defendant did and does store.

129. Defendant has a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of Defendant's relationship with them—especially to secure their PII.

130. Because of the highly sensitive nature of the PII, Plaintiff and Class Members would not have entrusted Defendant, or anyone in Defendant's position, to retain their PII had they known the reality of Defendant's inadequate data security practices.

131. Defendant breached its fiduciary duties to Plaintiff and Class Members by failing to sufficiently encrypt or otherwise protect Plaintiff's and Class Members' PII.

132. Defendant also breached its fiduciary duties to Plaintiff and Class Members by failing to diligently discover, investigate, and give notice of the Data Breach in a reasonable and practicable period.

133. As a direct and proximate result of Defendant's breach of its fiduciary duties, Plaintiff and Class Members have suffered and will continue to suffer numerous injuries (as detailed *supra*).

COUNT IV
Breach of Implied Contract
(On Behalf of Plaintiff and the Class)

134. Plaintiff and members of the Class incorporate the above allegations as if fully set forth herein.

135. Plaintiff and Class Members were required to provide their PII to Defendant as a

condition of receiving employment and/or educational services from Defendant. Plaintiff and Class Members provided their PII to Defendant in exchange for Defendant's employment and/or educational services.

136. Plaintiff and Class Members reasonably understood that a portion of the funds derived from their employment and/or a portion of the funds paid to Defendant via tuition payments for educational services would be used by Defendant used to pay for adequate cybersecurity and protection of their PII.

137. Plaintiff and the Class Members accepted Defendant's offers by disclosing their PII to Defendant in exchange for employment and/or educational services.

138. Plaintiff and Class Members entered into implied contracts with Defendant under which Defendant agreed to safeguard and protect such information and to timely and accurately notify Plaintiff and Class Members if and when their data had been breached and compromised. Each such contractual relationship imposed on Defendant an implied covenant of good faith and fair dealing by which Defendant was required to perform its obligations and manage Plaintiff's and Class Members' data in a manner which comported with the reasonable expectations of privacy and protection attendant to entrusting such data to Defendant.

139. In providing their PII, Plaintiff and Class Members entered into an implied contract with Defendant whereby Defendant, in receiving such data, became obligated to reasonably safeguard Plaintiff's and the other Class Members' PII.

140. In delivering their PII to Defendant, Plaintiff and Class Members intended and understood that Defendant would adequately safeguard that data.

141. Plaintiff and the Class Members would not have entrusted their PII to Defendant in the absence of such an implied contract.

142. Defendant accepted possession of Plaintiff's and Class Members' PII.

143. Had Defendant disclosed to Plaintiff and Class Members that Defendant did not have adequate computer systems and security practices to secure employees' and students' PII, Plaintiff and members of the Class would not have provided their PII to Defendant.

144. Defendant recognized that employees' and students' PII is highly sensitive and must be protected, and that this protection was of material importance as part of the bargain to Plaintiff and Class Members.

145. Plaintiff and Class Members fully performed their obligations under the implied contracts with Defendant.

146. Defendant breached the implied contract with Plaintiff and Class Members by failing to take reasonable measures to safeguard their data.

147. Defendant breached the implied contract with Plaintiff and Class Members by failing to promptly notify them of the access to and exfiltration of their PII.

148. As a direct and proximate result of the breach of the contractual duties, Plaintiff and Class Members have suffered actual, concrete, and imminent injuries. The injuries suffered by Plaintiff and the Class Members include: (a) the invasion of privacy; (b) the compromise, disclosure, theft, and unauthorized use of Plaintiff's and Class Members' PII; (c) economic costs associated with the time spent to detect and prevent identity theft, including loss of productivity; (d) monetary costs associated with the detection and prevention of identity theft; (e) economic costs, including time and money, related to incidents of actual identity theft; (f) the emotional distress, fear, anxiety, nuisance and annoyance of dealing related to the theft and compromise of their PII; (g) the diminution in the value of the services bargained for as Plaintiff and Class Members were deprived of the data protection and security that Defendant promised when Plaintiff

and the proposed class entrusted Defendant with their PII; and (h) the continued and substantial risk to Plaintiff's and Class Members' PII, which remains in the Defendant's possession with inadequate measures to protect Plaintiff's and Class Members' PII.

COUNT V
Invasion of Privacy
(On Behalf of Plaintiff and the Class)

149. Plaintiff and members of the Class incorporate the above allegations as if fully set forth herein.

150. Defendant publicized private details and facts not generally known to the public, not publicly available, and not of legitimate public concern about Plaintiff and the Class by disclosing and exposing Plaintiff's and Class's PII to enough people that it is reasonably likely those facts will become known to the public at large, including without limitation on the dark web and elsewhere.

151. Plaintiff and members of the Class had a legitimate expectation of privacy regarding their highly sensitive financial and personal information and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

152. Defendant owed a duty to employees and students, including Plaintiff and the Class, to keep this information confidential.

153. The disclosure of the PII, including employees' and students' names, Social Security numbers, , and driver's license information is particularly harmful and would be offensive to a reasonable person of ordinary sensibilities.

154. Defendant has extensive knowledge of its employees' financial standings and therefore has a special relationship with Plaintiff and the Class and Defendant's disclosure of PII is certain to embarrass them and offend their dignity. Defendant should appreciate that the cyber-

criminals who stole the PII would further sell and disclose the PII as they are doing. That the original disclosure is devastating to the Plaintiff and the Class, even though it originally may have only been disclosed to one person or a limited number of cyber-criminals, does not render it any less a disclosure to the public-at-large.

155. Defendant acted with a knowing state of mind when it permitted the Data Breach because it knew its information security practices were inadequate.

156. Defendant acted with a knowing state of mind when it failed to notify Plaintiff and the Class in a timely fashion about the Data Breach, thereby materially impairing their mitigation efforts.

157. Acting with knowledge, Defendant had notice and knew that its inadequate cybersecurity practices would cause injury to Plaintiff and the Class.

158. As a proximate result of Defendant's acts and omissions, the private and sensitive PII of Plaintiff and the Class were stolen by a third party and is now available to disclosure and redisclosure without authorization, causing Plaintiff and the Class to suffer damages.

159. Unless and until enjoined and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and the Class since those personal and financial records are still maintained by Defendant with their inadequate cybersecurity system and policies.

160. Plaintiff and the Class have no adequate remedy at law for the injuries relating to Defendant's continued possession of their sensitive and confidential medical records. A judgment for monetary damages will not end Defendant's inability to safeguard the medical records of Plaintiff and the Class. In addition to injunctive relief, Plaintiff, on behalf of herself and the other members of the Class, also seeks compensatory damages for Defendant's invasion of privacy,

which includes the value of the privacy interest invaded by Defendant, the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest, and costs.

COUNT VI
Unjust Enrichment
(On Behalf of Plaintiff and the Class)

161. Plaintiff and members of the Class incorporate the above allegations as if fully set forth herein.

162. This claim is pleaded in the alternative to the breach of implied contractual duty claim.

163. Plaintiff and Class Members conferred a monetary benefit on Defendant, by providing Defendant with their valuable PII.

164. Defendant enriched itself by saving the costs they reasonably should have expended on data security measures to secure Plaintiff's and Class Members' PII.

165. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant calculated to avoid its data security obligations at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and the Class, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide the requisite security.

166. Under the principles of equity and good conscience, Defendant should not be permitted to retain the monetary value of the benefit belonging to Plaintiff and Class Members, because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

167. Defendant acquired the monetary benefit and PII through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

168. If Plaintiff and Class Members knew that Defendant had not secured their PII, they

would not have agreed to provide their PII to Defendant.

169. Plaintiff and Class Members have no adequate remedy at law.

170. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) the loss of the opportunity how their PII is used; (ii) the compromise, publication, and/or theft of their PII; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fail to undertake appropriate and adequate measures to protect PII in their continued possession; and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and the Class.

171. As a direct and proximate result of Defendant's conduct, Plaintiff and the Class have suffered and will continue to suffer other forms of injury and/or harm.

172. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that they unjustly received from them.

PRAYER FOR RELIEF

Plaintiff and Class Members respectfully request judgment against Defendant and that the Court enter an order:

A. Certifying this case as a class action on behalf of Plaintiff and the proposed Class, appointing Plaintiff as class representative, and appointing his counsel to represent the Class;

B. Awarding declaratory and other equitable relief as necessary to protect the interests of Plaintiff and the Class;

C. Awarding injunctive relief as necessary to protect the interests of Plaintiff and the Class;

D. Enjoining Defendant from further unfair and/or deceptive practices;

E. Awarding Plaintiff and the Class damages including applicable compensatory, exemplary, punitive damages, and statutory damages, as allowed by law;

F. Awarding restitution and damages to Plaintiff and the Class in an amount to be determined at trial;

G. Awarding attorneys' fees and costs, as allowed by law;

H. Awarding prejudgment and post-judgment interest, as provided by law;

I. Granting Plaintiff and the Class leave to amend this complaint to conform to the evidence produced at trial; and

J. Granting other relief that this Court finds appropriate.

DEMAND FOR JURY TRIAL

Plaintiff demands a jury trial for all claims so triable.

Dated: May 12, 2025

Respectfully submitted,

/s/ David H. Fink
David H. Fink (P28235)
Nathan J. Fink (P75185)
FINK BRESSACK
38500 Woodward Ave., Suite 350

Bloomfield Hills, MI 48304
Telephone: (248) 971-2500
dfink@finkbressack.com
nfink@finkbressack.com

Raina C. Borrelli*
STRAUSS BORRELLI PLLC
980 N. Michigan Avenue, Suite 1610
Chicago, Illinois 60611
T: (872) 263-1100
F: (872) 263-1109
raina@straussborrelli.com

**Application for admission to be submitted*

Attorneys for Plaintiff and Proposed Class